



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,901	10/07/2005	Nicolas Gisin	GISIN1A	2392

1444 7590 12/05/2006

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER

DOAN, TRANG T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 12/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/534,901

Applicant(s)

GISIN ET AL.

Examiner

Trang Doan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 May 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 5-10 is/are rejected.
- 7) ☒ Claim(s) 4 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 May 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 05/2005.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are pending in this application.
2. The application is filed on 10/07/2005 but claims the benefit of Foreign Priority Application has been made and acknowledged. Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 11/15/2002.

Claim Objections

3. Claim 1 is objected to because of the following informalities: in lines 14-15, there is a line skip between "suitable" and "sets". Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 6 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
6. The claim is directed to a method for exchanging a secure cryptographic key for a quantum cryptography system employ no-ideal elementary quantum states, which is merely an arithmetic operation via a mathematical algorithm. The claim is not limited to a practical application of the mathematical algorithm because the result is not a useful, concrete and tangible result. More specifically the result is not a tangible result because it is not a real-world result.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 5, 7 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 1 recites the limitation "the analysis measurement" in line 13. There is insufficient antecedent basis for this limitation in the claim.

10. Claim 1 recites the limitation "the set information" in line 16. There is insufficient antecedent basis for this limitation in the claim.

11. Additionally to claim 1, the limitations "there is not single quantum operation reducing the overlap of the quantum states of all sets simultaneously" and "the receiver discards all received ...communication channel" lack meaning, in lines 9-10 and line 18 they are unclear as to how it relates to previous limitations.

12. Claim 5 recites the limitation "the public channel" in line 7. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 7 recites the limitation "the encoded bit" in page 5 line 12. There is insufficient antecedent basis for this limitation in the claim.

14. Claim 7 recites the limitation " the set information " in page 5 lines 13-14. There is insufficient antecedent basis for this limitation in the claim.

15. Claim 10 recites the limitation "one of the four pairs of non-orthogonal states $A(w, w')$ " in line 6-7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3 and 5-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Huttner et al. (Reference U) (hereinafter Hut).

3. Regarding claim 1, Hut teaches an emitter and a receiver, being connected by a quantum channel and a conventional communication channel (Hut: page 1863 column 2 lines 1-8 "In quantum cryptography...in the transmission"), the emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets (Hut: page 1863, lines 5-11 "in this technique...a potential eavesdropper" and page 1865, lines 1-4 "In this protocol... them deterministically"), there is no a single quantum operation reducing the overlap of the quantum states of all sets simultaneously (Hut: page 1865, left column "in the original proposal...as a phase reference" and right column "Let us now suggest..."), the emitter sends the encoded bit along the quantum channel to the receiver (Hut: page 1865, lines 1-8 "in this protocol...give the correct one"), the receiver randomly chooses the analysis measurement within said suitable sets (Hut: page 1865, left column "In this protocol...to this system"), the emitter sends

Art Unit: 2131

the set information along the conventional communication channel (Hut: page 1863, right column "In quantum cryptography...shortening their strings"), the receiver discards all received encoded bits for which he has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter along the conventional communication channel (Hut: page 1867, left column "The detection system...will be discarded" and page 1865, left column "in this protocol...to this system").

4. Regarding claim 2, Hut teaches wherein in the step of the emitter sending an encoded bit along the quantum channel to the receiver weak coherent states are exchanged between the emitter and the receiver (Hut: page 1865, right column "Alternative implementation" and page 1864, left column "At present...significantly increased").

5. Regarding claim 3, Hut teaches wherein the weak coherent states are laser pulses with an average photon number per pulse of less than 0.5 photons, preferably less than 0.1 photons (Hut: page 1868, left column "However...this is the task of sec. V" and "Lossy Transmission Line" section).

6. Regarding claim 5, Hut teaches wherein after a number of encoded bits has been transmitted, a protocol step is performed, within which emitter and receiver agree on a body of cryptographic key information which is shared between emitter and receiver, but secret from all other units who may be monitoring the quantum channel and the public channel, or else conclude that the encoded bits can not be safely used as cryptographic

key information (Hut: page 1866, left column "Safety of the two-states systems" section and page 1868, left column "Lossy Transmission Line" section).

7. Regarding claim 6, Hut teaches where the key values are encoded on at least two sets of non-orthogonal quantum states characterized by the fact that it is not possible to find a single quantum operation, whether probabilistic or not, that reduces the overlap of the states of all sets simultaneously (Hut: page 1865, left column "Two-States Protocol" section, page 1866, left column "Safety of the two-states systems" section and page 1868, left column "Lossy Transmission Line" section).

8. Regarding claim 7, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

9. Regarding claim 8, this claim has limitation that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

10. Regarding claim 9, this claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

11. Regarding claim 10, Hut teaches wherein for each bit, the emitter is randomly using one of the four states $|+x\rangle$ or $|+y\rangle$ with the convention that $|+x\rangle$ code for 0 and $|+y\rangle$ code for 1, and sends it along the quantum channel to the receiver (Hut: page 1864, left column "Four-States Protocol"), the receiver randomly measures σ_x or σ_y , the emitter announces one of the four pairs of non-orthogonal states $A(w, w') = \{|w\rangle, |w'\rangle$ with w, w' belong to $\{+, -\}$ and such that one of the states is the one which he has sent by sending an appropriate message along the conventional communication channel, the receiver discards all received encoded bits for which the

measurement result he has obtained is possible for both states disclosed by the emitter and sends an appropriate information to the emitter along the conventional communication channel, the receiver deduces the state actually sent by the emitter and adds the corresponding bit to the key (Hut: page 1864, left column "Four-States Protocol" and right column "Safety of four-states systems" section).

Allowable Subject Matter

12. Claim 4 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan
Examiner
Art Unit 2131

T.D.
11/21/2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100